IN THE CLAIMS

Listing of Claims:

1. (original) A method for ensuring a secure programming environment for a computer system comprising the steps:

modifying a processor of said computer system to incorporate an S-latch, a first state of said S-latch setting said processor in a secure state and a second state of said S-latch setting said processor in a non-secure state;

writing a security code in an NVRAM coupled to said computer system;

reading said security code from said NVRAM;

setting said first and second state of said S-latch in response to states of said security code; and

not accepting processor commands from an In Circuit Emulator (ICE) unit coupled to said computer system when said S-latch is in said first state and accepting processor commands from said ICE unit when said S-latch is in said second state.

2. (original) The method of claim 1, wherein said security code is read by boot block code within a Basic Input Output System (BIOS) code of said computer system.

3. (original) The method of claim 2, wherein said S-latch is set by said boot block code in response to reading said security code.

4. (original) The method of claim 2, wherein said boot block code is a first code executed on each power up or system reset of said computer system.

5. (currently amended) The method of claim 1, wherein said security code is encrypted when written into said NVRAM [[unit]].

6. (currently amended) The method of claim 1, wherein said security code is password protected when written into said NVRAM [[unit]].

7. (original) The method of claim 2, wherein said BIOS code is executed if said boot block code is able to authenticate said security code and said boot block code is able to

write to said S-latch if said security code corresponds to setting said first state of said S-latch.

8. (original) The method of claim 2, wherein said BIOS code is not executed if said boot block code is not able to authenticate said security code.

9. (original) The method of claim 2, wherein said BIOS code is not executed if said boot block code is able to authenticate said security code and said boot block code is not able to set a state of said S-latch.

10. (original) The method of claim 1, wherein said ICE unit is coupled to said computer system on a system bus of said computer system.

11. (original) The method of claim 1, wherein said ICE unit is coupled to said computer system on a JTAG scan chain bus.

12. (original) The method of claim 1, wherein said ICE unit is coupled to said computer system in place of said modified processor.

13. (original) The method of claim 1, wherein a default said S-latch in said computer system is set to a non-secure state.

14. (currently amended) A computer system comprising:

a central processing unit (CPU);

a random access memory (RAM);

non-volatile RAM (NVRAM);

a communications adapter coupled to a communication network;

an I/O adapter;

a bus system coupling said CPU to said NVRAM, said communications adapter, said I/O adapter, and said RAM, wherein said CPU further comprises:

a modified processor with an S-latch, a first state of said S-latch setting said modified processor in a secure state and a second state of said S-latch setting said modified processor in a non-secure state;

first circuitry operable to receive and write a security code in said NVRAM;

second circuitry operable to read said security code from said NVRAM~~; and~~

~~circuitry~~ and operable to set said first and second state of said S-latch in response to states of said security code;

wherein said modified processor accepts commands from an In Circuit Emulator (ICE) unit coupled to said computer system when said S-latch is in said second state and does not accept processor commands from said ICE unit when said S-latch is in said first state.

15. (original) The computer system of claim 14, wherein said security code is read by boot block circuitry within Basic Input Output System (BIOS) circuitry of said computer system.

16. (original) The computer system of claim 15, wherein said S-latch is set by said boot block circuitry in response to reading said security code.

17. (original) The computer system of claim 15, wherein said boot block circuitry reads said security code as a first operation on each power up or system reset of said computer system.

18. (currently amended) The computer system of claim 14, wherein said security code is encrypted when written into said NVRAM [[unit]].

19. (currently amended) The computer system of claim 14, wherein said security code is pass word protected when written into said NVRAM [[unit]].

20. (original) The computer system of claim 15, wherein said BIOS circuitry is enabled if said boot block code is able to authenticate said security code and said boot block code

is able to write to said S-latch if said security code corresponds to setting said first state of said S-latch.

21. (original) The computer system of claim 15, wherein said BIOS circuitry is disabled if said boot block is not able to authenticate said security code.

22. (original) The computer system of claim 15, wherein said BIOS circuitry is disabled if said boot block circuitry is not able to set said S-latch into a state.

23. (original) The computer system of claim 14, wherein said ICE unit is coupled to said computer system on a system bus of said computer system.

24. (original) The computer system of claim 14, wherein said ICE unit is coupled to said computer system on a JTAG scan chain bus.

25. (original) The computer system of claim 14, wherein said ICE unit is coupled to said computer system in place of said modified processor.

26. (original) The computer system of claim 14, wherein a default said S-latch in said computer system is set to a non-secure state.